MultiBio700 User Manual

Version: 1.0
Date: Oct. 2010

About This Manual

This document introduces the user interface and menu operations of MultiBio700. For the installation please refer to *Installation Guide.*

TABLE OF CONTENTS

1. INSTRUCTION FOR USE 1

1.1 STANDING POSITION, POSTURE AND FACE EXPRESSION 1
1.2 ENROLLMENT FACE EXPRESSION 2
1.3 FINGER PLACEMENT 3
1.4 USE OF TOUCH SCREEN 4
1.5 TOUCH OPERATIONS 5
1.6 APPEARANCE OF DEVICE 7
1.7 MAIN INTERFACE 8
1.8 VERIFICATION MODES 10
1.8.1 Fingerprint Verification 10
1.8.2 Face Verification 12
1.8.3 Password Verification 13
1.8.4 ID Card Verification ★ 14
1.8.5 Combination Verification ★ 15

2. MAIN MENU 17

3. ADD USER 19

3.1 ENTERING A USER ID 20
3.2 ENTERING A NAME 21
3. 3 ENROLLING A FINGERPRINT 22
3. 4 ENROLLING A PASSWORD 24
3. 5 ENROLLING A FACE 25
3.6 ENTERING A GROUP NO. 26
3.7 MODIFY USER RIGHTS 28
3.8 ENROLL PHOTOS 29
3.9 USER ACCESS SETTING 30

3.10 ENROLLING AN ID CARD ★ 33

4. USER MANAGEMENT 34

4.1 EDIT A USER 35
4.2 DELETE A USER 36
4.3 QUERY A USER 37

5. COMMUNICATION SETTINGS 38

5.1 NETWORK SETTINGS 39
5.2 WIEGAND OUTPUT 41
5.2.1 Wiegand 26-bits Output Description 42
5.2.2 Wiegand 34-bits Output Description 44
5.2.3 Customized Format 46
5.3 WIEGAND INPUT 50

6. SYSTEM CONFIGURATION 51

6.1 GENERAL PARAMETERS 52
6.2 INTERFACE PARAMETERS 53
6.3 FINGERPRINT PARAMETERS 54
6.4 FACE PARAMETERS 56
6.5 LOG SETTINGS 58
6.6 KEYBOARD DEFINITIONS 59
6.7 ACCESS SETTING 60
6.7.1 Time zone setting 61
6.7.2 Holiday setting 62
6.7.3 Group time zone setting 64
6.7.4 Unlock Combination Setting 67
6.7.5 Access control parameter 69
6.7.6 Duress alarm parameter 71

6.7.7 Anti-Pass back setting 72
6.8 UPDATE 73
7. DATA MANAGEMENT 74
8. DATE/TIME SETTING 77
8.1 SET DATE/TIME 77
8.2 BELL SETTING ★ 78
9. AUTO TEST 80
10. USB DISK MANAGEMENT 82
11. SYSTEM INFORMATION 83
12. APPENDIX 84
APPENDIX 1 T9 INPUT INSTRUCTIONS 84
APPENDIX 2 INTRODUCTION OF WIEGAND 86
APPENDIX 3 PHOTO ID FUNCTION 88
APPENDIX 4 MULTI-COMBINATION AUTHENTICATION MODE ★ 89
APPENDIX 5 ANTI-PASS BACK ★ 93
APPENDIX 6 STATEMENT ON HUMAN RIGHTS AND PRIVACY 96
APPENDIX 7 ENVIRONMENT-FRIENDLY USE DESCRIPTION 98

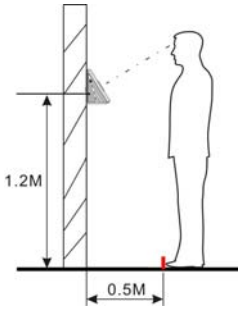
1. Instruction for Use

1.1 Standing Position, Posture and Face Expression

1. Recommended standing-distance from device:

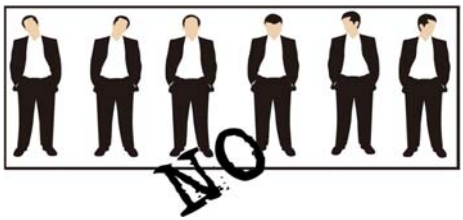
For users 5-6 feet tall (1.5m-1.85m) we recommend users stand about 2 feet (0.5m) from the wall.

When viewing your image on the device display window, step away if your image appears too bright. Step closer if your image appears too dark.



2. Recommended face Expressions vs. poor Expressions:

3. Recommended Posture (pose) vs. poor Posture (pose):



✍ **Note:** During enrollment and verification, try to have a relaxed unstrained face expression and stand upright.

1.2 Enrollment Face Expression

During the enrollment, position your head such that your face appears in the center of the device display window. The device will prompt you how to move your head.

Follow the voice prompts by first gently turning your head left, then right. Then your head gently down, then up , and so on. There slight variations of head angles will help the device better recognize your face when you attempt verifying:

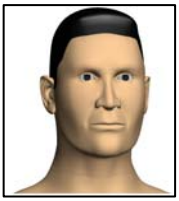
The enrollment face experssion as follows:

Look ahead

Look at screen

Bow down

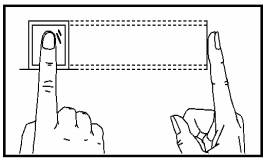
Turn left


Turn right

1.3 Finger Placement

Recommended fingers: The index finger, middle finger or the ring finger; the thumb and little finger are not recommended (because they are usually clumsy on the fingerprint collection screen).

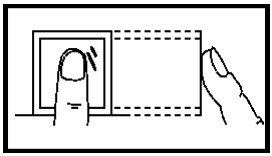
1. Proper finger placement:



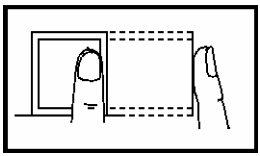
The finger is flat to the surface and centered in fingered guide.

2. Improper finger placement:

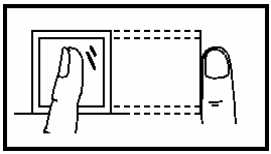
Not flat to the surface



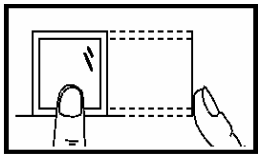
Off-center



Slanting



Off-center



Please enroll and verify your fingerprint by using the proper finger placement mode. We shall not be held accountable for any consequences arising out of the degradation in verification performance due to improper user operations. We shall reserve the right of final interpretation and revision of this document.

1.4 Use of Touch Screen

Touch the screen with one of your fingertips or the top of the forward edge of a fingernail, as shown in the following figure. A broad point of contact may lead to inaccurate pointing.

When the touch screen is less sensitive to the touch, you can perform screen calibration through menu operations. Press [**Menu**] -> [**Auto Test**] -> [**Calibration**] on the screen and a cross icon will be displayed. After you touch the center of the cross at five locations on the screen correctly, the system automatically returns to the main menu. Press [**Exit**] to return to the initial interface. For details, see the description in 9. Auto Test.

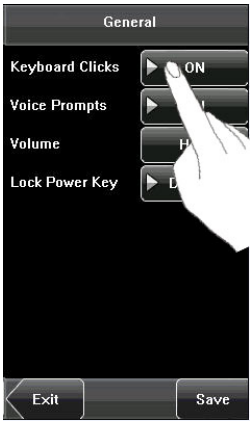
Smear or dust on the touch screen may affect the performance of the touch screen. Therefore, try to keep the screen clean and dust-free.

1.5 Touch Operations

1. Enter numbers: Press the [User ID] key. The system automatically displays the number input interface. After entering the user ID, press [OK] to save or press [X] to cancel and return to the previous interface.

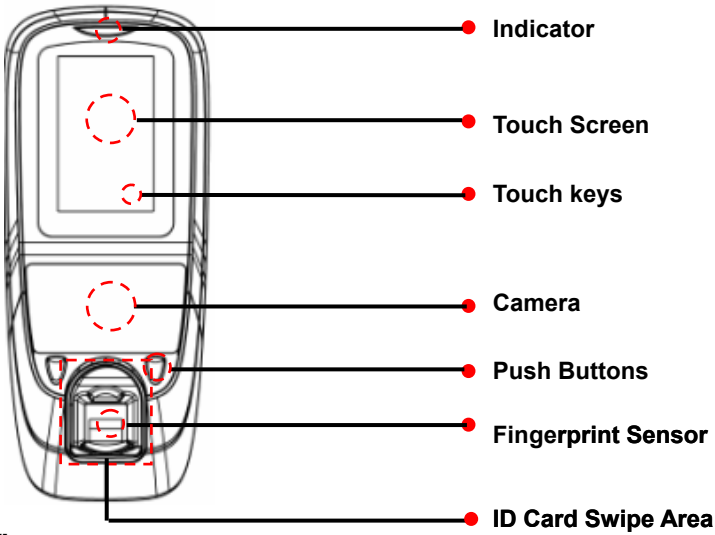
2. Enter Text: Press the [Name] key. The system automatically displays the text input interface. After entering the user name, press [X] to save and return to the previous interface.

3. Modify parameters: Press the default value of a parameter and the system automatically switches to another value of this parameter.

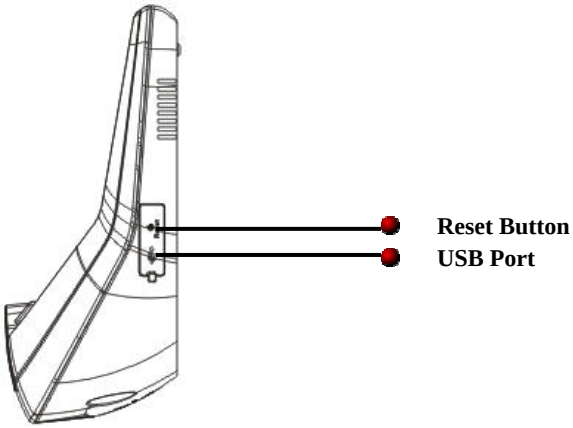


1.6 Appearance of Device

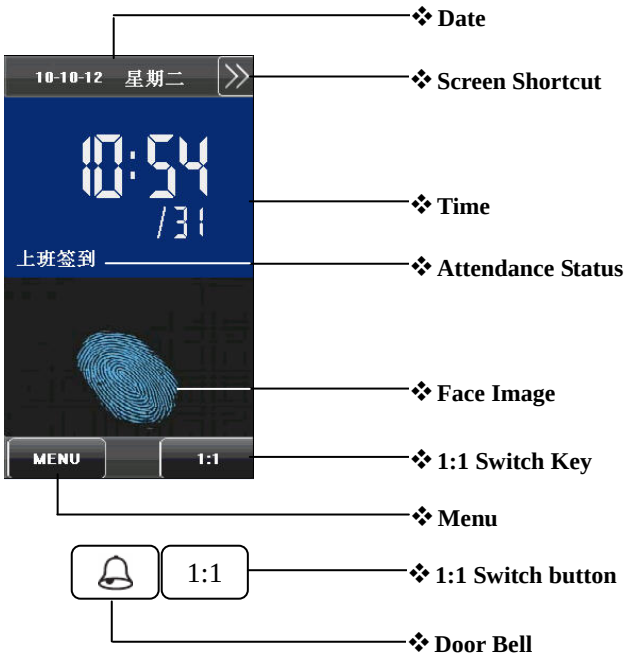
1.Front View



2.Side View



1.7 Main Interface



① **Date**: Current date is displayed.

② **Screen Shortcut Keys**: Press this shortcut keys to display the attendance status and enter the functional interface quickly. Users can customize the function of each shortcut key. For details, see 6.6 Keyboard Definitions.

③ **Time**: Current time is displayed. Both the 12-hour and 24-hour time systems are supported.

④ **Attendance Status**: Current attendance status is displayed.

⑤ **Fingerprint Image**: When the fingerprint image is displayed, the device is

currently in the fingerprint recognition mode.

⑥ **1:1 Switch Key**: By pressing this key, you can switch to the 1:1 verification modes, and enter the digital input interface. The function is same to ⑨[1:1] Switch Button.

⑦ **Menu**: You can enter the main menu by touching this key.

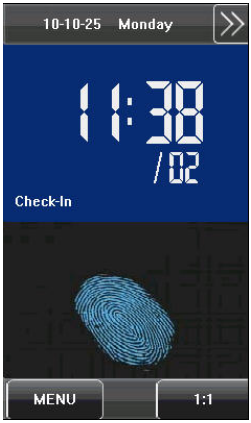
⑧ **Door Bell:** For guest to ring the bell and ask for opening the door.

⑨ **1:1 Switch Button:** You can enter the digital input interface of 1:1 verification mode.

1.8 Verification Modes

1.8.1 Fingerprint Verification

1. 1:N fingerprint verification



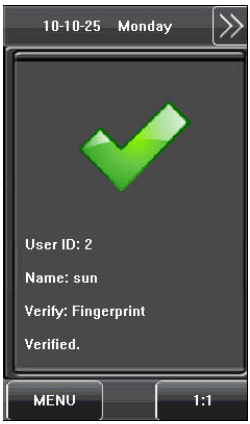
In the fingerprint verification mode, the device compares current fingerprint collected by the fingerprint collector with all fingerprint data on the device.

1. The default main interface is the fingerprint verification mode, see the figure on the right.

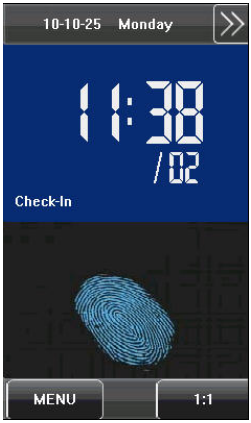
2. Press your finger on the fingerprint collector by adopting the proper finger placement. For details, see 1.3 Finger Placement.

3. If the verification is successful, the device prompt "Verified".

4. If the verification is not successful, the device prompt "Please try again".



2. 1:1 fingerprint verification



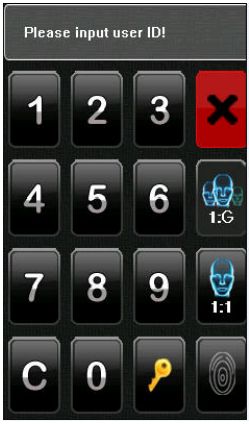
In the 1:1 fingerprint verification mode, the device compares current fingerprint collected through the fingerprint collector with that in relation to the user ID entered through keyboard. Adopt this mode only when it is difficult to recognize the fingerprint.

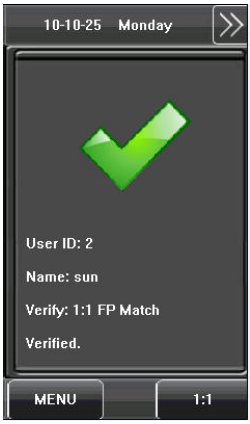
1. Press [1:1] on the screen or [1:1] keyboard to enter the 1:1 fingerprint recognition mode.

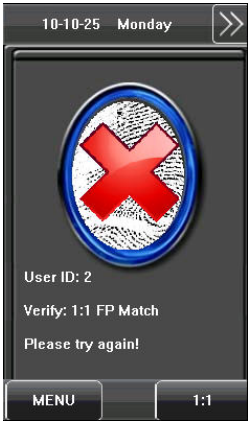
2. Enter user ID and then press the "Fingerprint" icon to enter 1:1 fingerprint recognition mode. If the prompt “Unregistered user!” is displayed, the user ID is not exist.

3. Press your finger on the fingerprint collector by adopting the proper finger placement. For details, see 1.3 Finger Placement.

4. If the verification is successful, , the device prompt “Verified”, otherwise the device prompt “Please try again”.

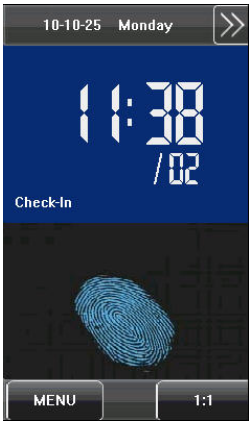






1.8.2 Face Verification

1:1 face verification



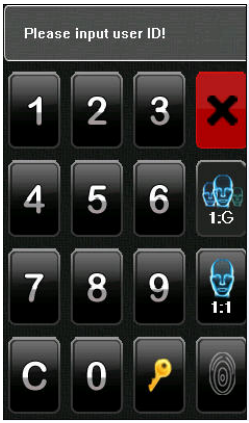
In the 1:1 face verification mode, the device compares current face collected through the camera with that in relation to the user ID entered through keyboard. Adopt this mode only when it is difficult to recognize the face.

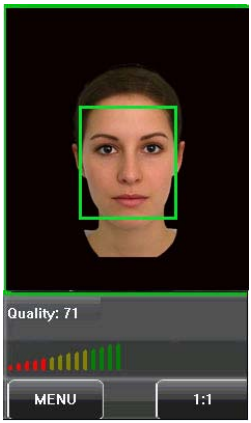
1. Press [1:1] on the screen or [1:1] keyboard to enter the 1:1 recognition mode.

2. Enter user ID and then press the "1:1 Face" icon to enter 1:1 face recognition mode. If the prompt “Unregistered user!” is displayed, the user ID is not exist.

3. Compare the face in a proper way. For details, see 1.1 Standing Position, Posture and Face Expression.

4. If the verification is successful, the device prompt “Verified”. The system will return to the main interface if the verification is not passed within 20 seconds.

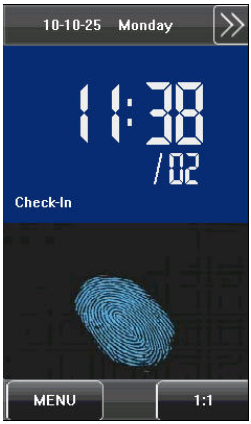


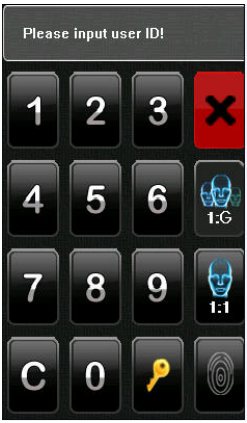


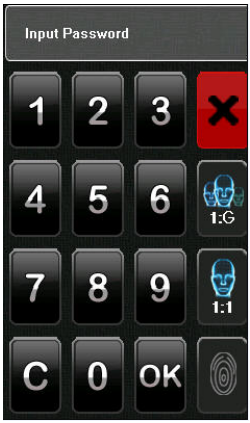
1.8.3 Password Verification

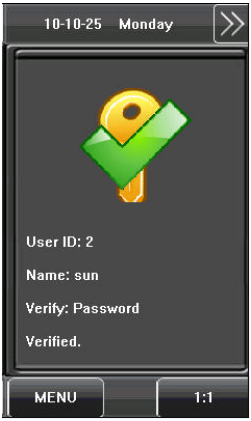
In the password verification mode, the device compares the password entered with that in relation to the user ID.

1. Press [1:1] on the screen or [1:1] keyboard to enter the password verification mode.
2. Enter the user ID and then press the "Key" icon to enter password verification mode. If the prompt "Unregistered user!" is displayed, the user ID is not exist.
3. Enter the password and press the "OK" icon to start the password comparison.
4. If the verification is successful, the device prompt "Verified", otherwise the device prompt "Verify fail" and return to password input interface.



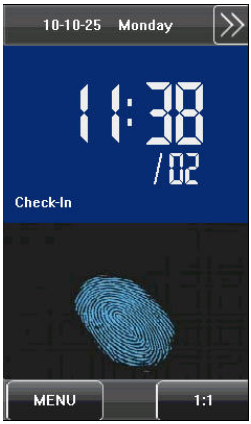






1.8.4 ID Card Verification ★

Note: Only the products with a built-in ID card module support the ID card verification.

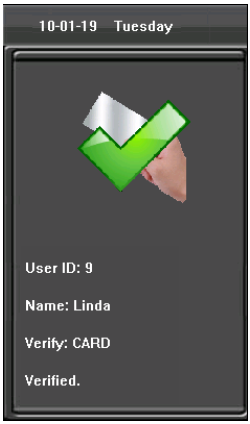


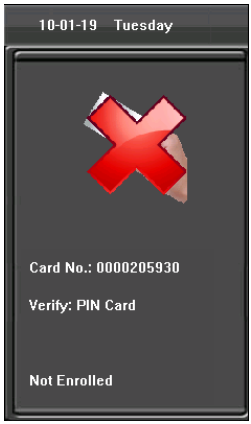
In the fingerprint verification mode, the device compares current ID Card collected by the Card Reader with all ID Card data on the device.

1. Swipe your ID Card on the Card Swipe Area by adopting the proper way. For the Card Swipe Area, see 1.6 Appearance of Device.

3. If the verification is successful, the device prompt "Verified".

4. If the verification is not successful, the device prompt "Card not Registered".





1.8.5 Combination Verification ★

The device support 20 verification modes, including FACE&PIN/FP/RF/PW、FP&PW、FP&RF、FACE&FP、FACE&PW、FACE&RF、FP、PW、RF、FACE&PIN、FP/RF、PW/RF、FP/PW、PW&RF、PIN&FP、FP&PW&RF、PIN&FP&PW、FP&RF/PIN、FACE&FP&RF、FACE&FP&PW etc. For the detail, please refer to Appendix 4 Multi-combination Authentication Mode.

Note: RF means ID Card verification. Only the products with a built-in ID card module support the ID card verification.

Here is the combination verification operation, we use the FACE&FP verification for an example.

If you verify fingerprint first and then the face verify, operation as follows.

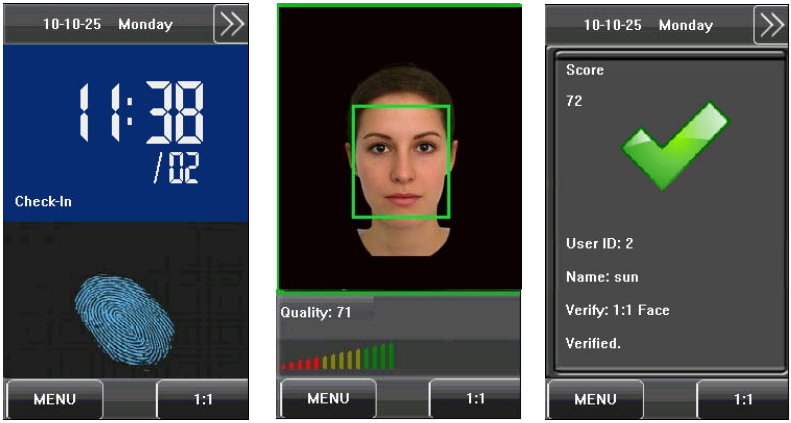
(1) The default main interface is the fingerprint verification mode, see the figure below.

(2) Press your finger on the fingerprint collector by adopting the proper finger placement. For details, see 1.3 Finger Placement.

(3) If the verification is successful, the device enter the 1:1 face recognition mode.

Compare the face in a proper way. For details, see 1.1 Standing Position, Posture and Face Expression.

(4) If the verification is successful, the device prompt “Verified”. The system will return to the main interface if the verification is not passed within 20 seconds.



Otherwise, the FACE&FP combination verification can perform such as FACE(1:N)+FP, PIN+FACE(1:1)+FP, PIN+FP(1:1)+FACE etc. The operation is similar to the procedure introduced before.

2. Main Menu

There are two types of rights respectively granted to two types of users: the **Ordinary users** and **administrators**. Ordinary users are only granted the rights of face, fingerprint, password or card verification, while administrators are granted the access to the main menu for various operations apart from having all the privileges granted to ordinary users.

Press [**Menu**] on the initial interface to access the main menu, as shown in the following figure:

The main menu includes nine submenus:

Add User: Through this submenu, you can add a new user and input the information on the device, including the user ID, name, fingerprint, face, card, password, rights, group No. and user access.

User Mgt.: Through this submenu, you can browse the user information stored on the device, including the user ID, name, fingerprint, face, card, password, rights, group No. and user access. And add, modify or delete the user information.

Comm.: Through this submenu, you can set related parameters for communication between the device and PC, including the IP address, gateway, subnet mask, baud rate, device No. and communication password.

System: Through this submenu, you can set system-related parameters, including the basic parameters, interface parameters, fingerprint, face and attendance parameters, Keyboard definitions, Access setting, firmware update etc. to enable the device to meet user requirements to the greatest extent in terms of functions and display.

Data Mgt.: Through this submenu, you can perform management of data stored on the device, for example, deleting the attendance record, all data, clear administrator, restore to factory settings and query records.

Date/Time: Through this submenu, you can set the alarm time and duration, or set the Bell.

Auto Test: This submenu enables the system to automatically test whether functions of various modules are normal, including the screen, collector, voice, face, keyboard, clock tests and screen calibration.

Dn/Upload: Through this submenu, you can import user information and attendance data stored in the device through a USB disk to related software or other fingerprint recognition equipment.

Sys Info.: Through this submenu, you can browse the records and device information.

Any user can access the main menu by pressing the [**Menu**] key if the system is free from administrators. After administrators are configured on the device, the device needs to verify the administrators' identity before granting them access to the main menu. To ensure device security, it is recommended to set an administrator when using the terminal initially. For detailed operations, see 3.7 Modify User Rights .

3. Add User

Press [Add] on the [User Mgt.] interface to display the [Add User] interface as shown below.

User ID: Enter a user ID. 1 to 9 digits user IDs are supported by default.

Name: Enter a user name. 12 characters user names are supported by default.

Fingerprint: Enroll a user's fingerprint and the Device displays the number of enrolled fingerprints. A user can enroll 10 fingerprints at maximum.

Password: Enroll a user's password. 1 to 8 digits passwords are supported by default.

Face: Enroll a user's face.

Group No.: Set the group that the user belongs to. Valid group No.: 1–24.

Role: Set the rights of a user. A user is set to **ordinary user** by default and can also be set to **administrator**. Ordinary users are only granted the rights of face, fingerprint or password verification, while administrators are granted the access to the main menu for various operations apart from having all the privileges granted to ordinary users.

Photo: Enroll a user's photo. During user verification, the user's photo is displayed on screen.

User Access: Set the lock control and access control parameters.

3.1 Entering a User ID

The device automatically allocates an ID starting from 1 for every user in sequence. If you use the ID allocated by the device, you may skip this section.

1. Press [User ID] on the [Add User] interface to display the user ID management interface.

Tip: The user ID can be modified during initial enrollment, but once enrolled, it cannot be modified.

2. On the displayed keyboard interface, enter a user ID and press [OK]. If a prompt message “The user ID already exists!” is displayed, enter another ID.

Tip: The device supports 1 to 9 digits user IDs by default. If you need to extend the length of current user ID numbers, please consult our commercial representatives or fore-sale technical support personnel.

3. After the user ID is entered, press [Save] to save current information and return to the previous interface. Press [Exit] to return to the previous interface without saving current information.

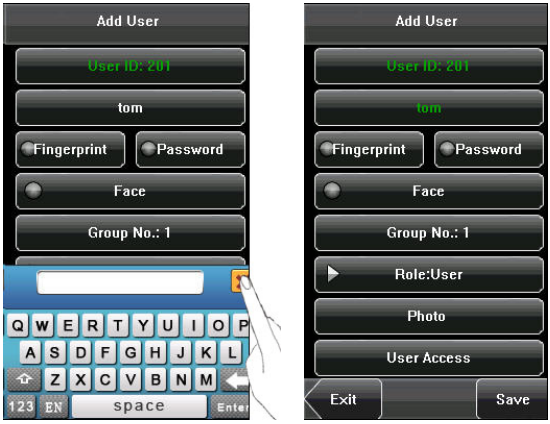
3.2 Entering a Name

Use T9 input method to enter the user name through the keyboard.

1. Press [Name] on the [Add User] interface to display the name input interface.
2. On the displayed keyboard interface, enter a user name and press [X].

For details of operations on keyboard interface, see Appendix 1 T9 Input Instructions.

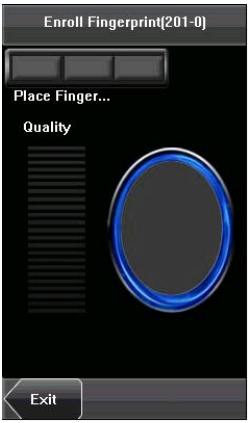
3. After the user name is entered, press [Save] to save current information and return to the previous interface. Press [Exit] to return to the previous interface without saving current information.



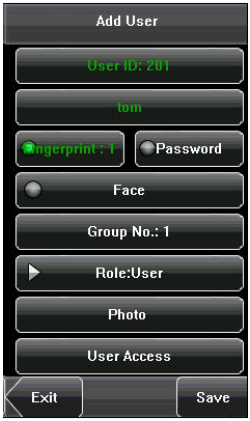
Tip: The device supports the 1 to 12 characters names by default.

3. 3 Enrolling a Fingerprint

1. Press [Fingerprint] on the [Add User] interface to display the [Enroll Fingerprint] interface.
2. On the displayed [Enroll Fingerprint] interface, place your finger on the fingerprint collector properly according to the system prompt. For details, see 1.3 Finger Placement.
3. Place the same finger on the fingerprint collector for three consecutive times correctly. If the enrollment succeeds, the system will display a prompt message and automatically return to the [Add User] interface. If the enrollment fails, the system will display a prompt message and return to the [Enroll Fingerprint] interface. In this case, you need to repeat the operations of step 2.
4. You can back up the enrolled fingerprint of a user by pressing [Fingerprint]. A user can enroll 10 fingerprints at maximum.
5. Press [Save] to save current information and return to the previous interface. Press [Exit] to return to the previous interface without saving current information.


Enroll Fingerprint(201-0)
Place Finger...
Quality
Exit

Enroll Fingerprint(201-0)
Enrolled Successfully
Quality 70
Exit

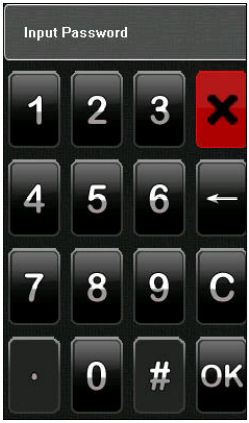

Add User
User ID: 201
tom
Password
Face
Group No.: 1
Role:User
Photo
User Access
Exit
Save

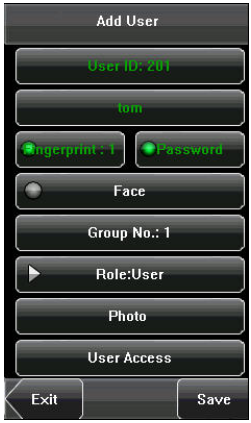
3. 4 Enrolling a Password

1. Press [Password] on the [Add User] interface to display the password management interface.
2. On the displayed keyboard interface, enter a password and press [OK]. Re-enter the password according to the system prompt and then press [OK].

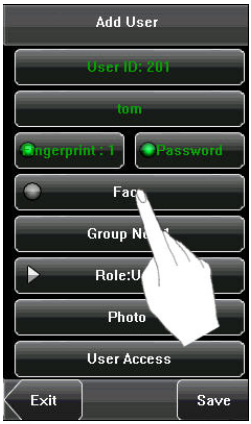
Tip: The device supports the 1 to 8 digits passwords by default.

3. After the password is entered, an interface is displayed as shown below. Press [Save] to save current information and return to the previous interface. Press [Exit] to return to the previous interface without saving current information.





3. 5 Enrolling a Face

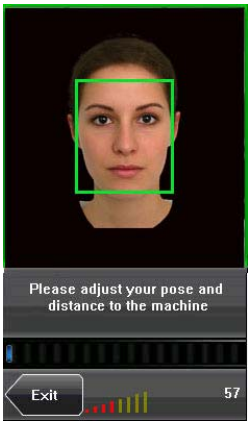


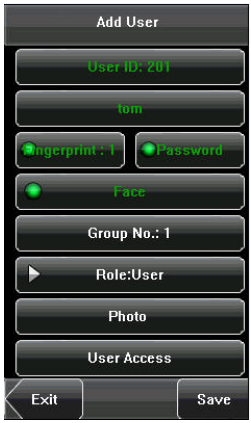
1. Press [Face] on the [Add User] interface to display the face enrollment interface.

2. On the displayed face enrollment interface, turn your head to the left and right slightly, raise and lower your head according to the voice prompts, so as to enroll different parts of your face into the system to assure accurate verification. See 1.2 Enrollment Face Expression.

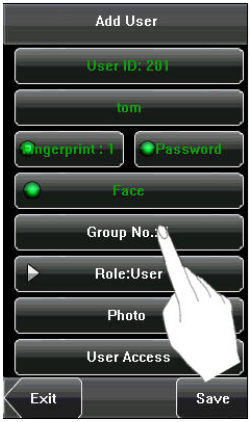
3. If your face image is enrolled successfully, the system will display a prompt message and automatically return to the [Add User] interface.

4. Press [Save] to save current information and return to the previous interface. Press [Exit] to return to the previous interface without saving current information.





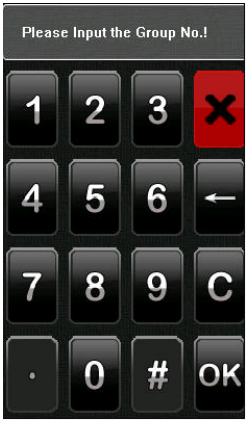
3.6 Entering a Group No.

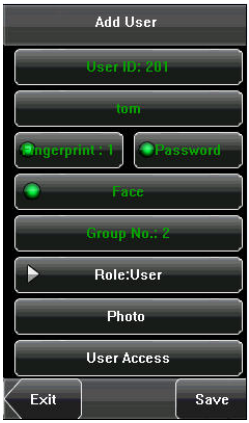


During face enrollment, the device automatically allocates a group No. starting from 1 for every user in sequence. When the number of users in Group No.1 reaches the upper limit, the rest users fall under Group No.2 automatically. Up to 100 face images can be enrolled in Group No.1 and only 50 face images can be enrolled in other groups. If you use the group No. allocated by the device, you may skip this section.

1. Press [Group No.] on the [Add User] interface to display the group No. management interface.
2. On the displayed keyboard interface, enter your group No. and press [OK].
3. After the group No. is entered, an interface is displayed as shown below. Press [Save] to save current information and return to the previous interface. Press [Exit] to return to the previous interface without saving current information.

✍ **Tip:** A valid group No. contains 1–24 digits. Please remember your own group No.


Please Input the Group No.!
1
2
3
4
5
6
7
8
9
C
0
#
OK


Add User
User ID: 201
tom
Fingerprint : 1
Password
Face
Group No.: 2
Role:User
Photo
User Access
Exit
Save

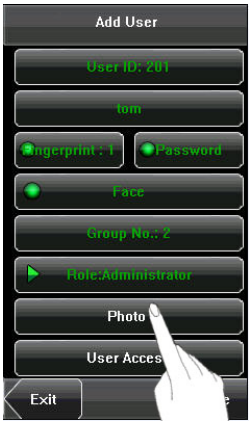
3.7 Modify User Rights

✍ **Note:** There are two types of rights respectively granted to two types of users: the **ordinary users** and **administrators**. Ordinary users are only granted the rights of face, fingerprint, or password verification, while administrators are granted the access to the main menu for various operations apart from having all the privileges granted to ordinary users.

1. On the [Add User] interface, press [Role: User] to change the user into an administrator.

2. After the modification is done, the interface is as shown below. Press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.

3.8 Enroll Photos



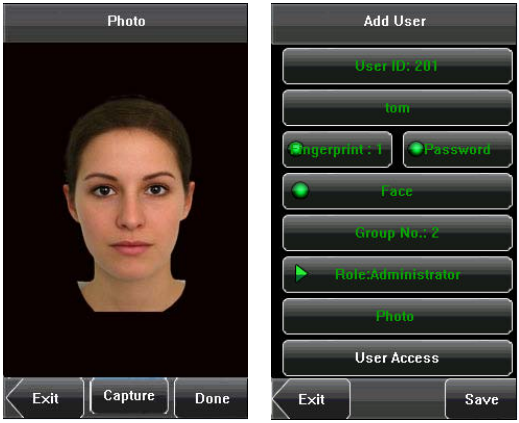
If you have enrolled your photo in the system, the system will display your enrolled photo in addition to your ID and name after you pass the verification.

1. Press [Photo] on the [Add User] interface to display the photo enrollment interface.

2. On the photo enrollment interface, stand naturally in front of the screen. For details, see 1.1 Standing Position, Posture and Face Expression. Press [Capture] to capture the photo.

3. After taking the photo, press [Exit] to return to previous interface.

4. After the photo is taken, press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.



3.9 User Access Setting

Press [User Access] on the [Add User] interface to display the user access setting interface.

User Access setting is to set the user right to verify and open the door. Including Verify Type, Time Zone and Duress FP management.

1. Verify Type:

(1) Group Verify Mode: If the user use the group verify mode that he belong to.

(2) Individual verify mode: Select the verify mode for this user instead of the group verify mode. That will not effect the other user in the group.

Note:

(1) Only the products with a built-in ID card module support the ID card verification.

(2) For the verify type, please refer to Appendix 4 Multi-combination Authentication Mode. Only some type of device support Multi-combination authentication mode.

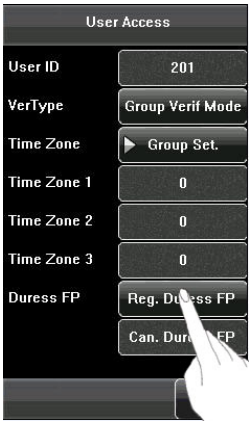
2. Time Zone:

(1) Group Time Zone: If the user use the group time zone that he belong to.

(2) Individual time zone: Select the time zone of this user instead of the group time zone. That will not effect the other user in the group.

3. Duress FP:

Enroll a new duress fingerprint or cancel an exist one. In any situation, only if the enrolled duress fingerprint is verified, it will trigger the duress alarm.



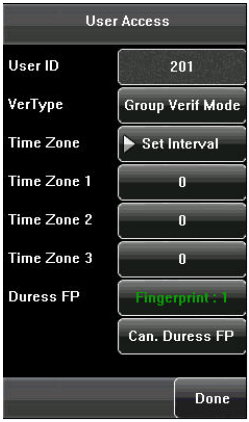
Duress FP management:

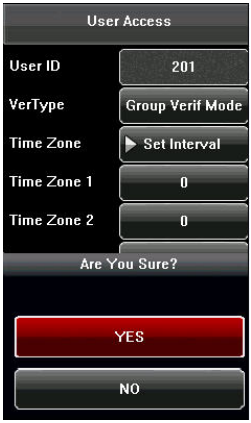
(1) Register Duress FP:

Press [Reg. Duress FP] on the [User Access] interface to display the [Enroll Fingerprint] interface. On the displayed [Enroll Fingerprint] interface, place your finger on the fingerprint collector properly according to the system prompt. For details, see 1.3 Finger Placement.

(2) Cancel duress FP:

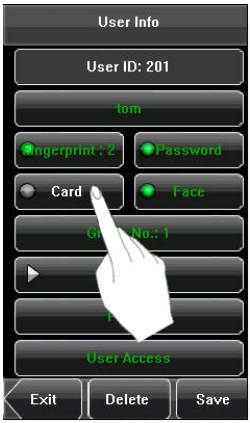
Press [Can.Duress FP] on the [User Access] interface to popup the confirm message. Select [YES] to delete the enrolled duress FP, otherwise select [NO] to cancel the operation.

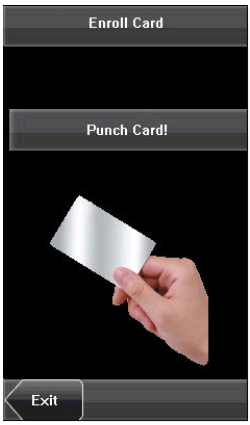


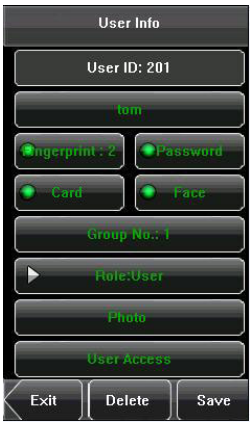


3.10 Enrolling an ID Card ★

1. Press [Card] on the [Add User] interface to display the [Enroll Card] interface.
2. The [Punch Card!] interface pops out as shown below. Swipe your ID card properly in the swiping area. For details, see 1.6 Appearance of the Device.
3. If the card passes the verification, the Device displays a prompt message "Read Successfully! Card No.: **********", and returns to the [Add User] interface.
4. Press [Save] to save current information and return to the previous interface. Press [Exit] to return to the previous interface without saving current information.





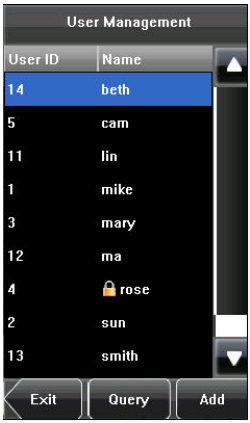


4. User Management

Browse the user information, including the user ID, name, fingerprint, face, ID card, password, rights, group No. and user access settings. To add, edit or delete the basic information of users.

Press [User Management] on the main menu interface to display the user management interface.

The user is an administrator.



Note: The users are listed in alphabetical order by last name. If you select a user, you can access the editing interface of this user to edit or delete related user information.

4.1 Edit a User

Select a user from the list to enter [User Info] interface.

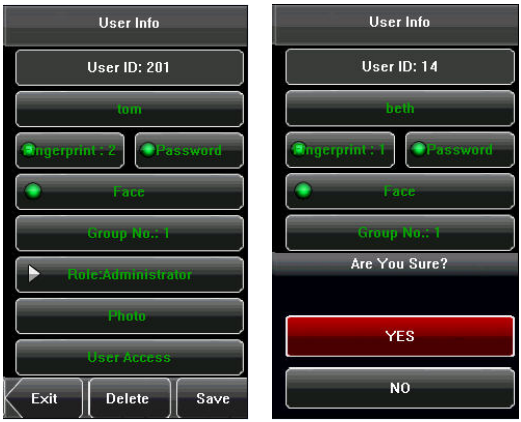
The User ID cannot be modified, and the other operations are similar to those performed to add a user. You can re-enroll your fingerprint and face image, change your password and modify the management rights and group No.

For example: Change the user right from Administrator to ordinary user. As the figure shown below.

4.2 Delete a User

On the [User Info] interface, you can delete all or partial user information.

1. Press [Delete] to delete a user.
2. On the interface displayed, click [YES] to delete current user and [NO] to return to previous interface.
3. On the [User Info] interface, press [Name], [Fingerprint], [Face] or [Password] to delete related user information and re-enroll the new information follow the device prompt.

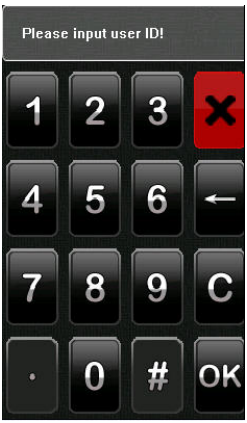


4.3 Query a User

To facilitate administrators to locate a user quickly from a large number of enrolled users, the Device enables user query by his/her “User ID”.

User ID Query:

1. Press [Query] on the [User Management] interface to display the User ID query interface.
2. Enter the user ID on the displayed interface, and click [OK] to locate the cursor to the desired user.



5. Communication Settings

You can set related parameters for the communication between the Device and PC, including the IP address, gateway, subnet mask, baud rate, equipment ID, and communication password.

5.1 Network Settings

When the Device communicates with the PC over **Ethernet**, you need to check the following settings:

IP Address: The IP address is 192.168.1.201 by default and can be changed as required; the IP address of the Device and that of the PC cannot be duplicated.

Subnet Mask: The subnet mask is 255.255.255.0 by default and can be changed as required.

Gateway: The gateway is 0.0.0.0 by default. If the Device and the PC are not located in the same network segment, you need to set the gateway.

When the Device communicates with the PC over **serial ports (RS232/RS485)**, you need to check the following settings:

RS232: This parameter is used to enable or disable the RS232 communication. If the RS232 communication cables are used, set this parameter to “ON”.

RS485: This parameter is used to enable or disable the RS485 communication. If the RS485 communication cables are used, set this parameter to “ON”.

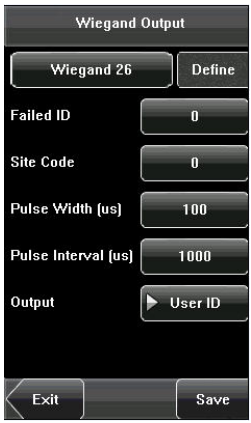
Baud Rate: This parameter is used to set the baud rate for the communication between the Device and the PC. It includes five options: 9600, 19200, 38400, 57600, and 115200. The high baud rate is recommended for the RS232 communication to achieve high communication speed, while the low baud rate is recommended for the RS485 communication to achieve stable low-speed communication.

Device ID: This parameter is used to set the ID of device from 1 to 254. If the RS232/RS485 communication is adopted, you need to enter the device ID on the software communication interface.

Comm. Key: To enhance the security of attendance data, you can set a password for the connection between the Device and PC. Once the password is set, you can connect the PC with the Device to access the attendance data only after entering the correct password. The default password is 0 (that is, no password). Once a password is set, you need to enter this password before connecting the PC software with the Device; otherwise, the connection is unsuccessful. 1 to 6 digits passwords are supported.

Considering the massive data including the fingerprint and face templates stored in the device, it is recommended to transfer the data between the device and PC over network to enhance the transfer speed.

5.2 Wiegand Output



Wiegand Format: The system has two built-in formats **Wiegand 26-bits** and **Wiegand 34-bits**, and also supports the format customization function to meet individualized requirements.

Failed ID: Refers to the value output by the system upon verification failure. The output format is subject to the setting of "**Wiegand Format**". The default value scope of **Failed ID** is 0–65535.

Site Code: The site code is used for customized Wiegand format. The site code is similar to the device ID, but the site code is customizable and can be duplicated among different devices. The default value scope of the site code is 0–255.

Pulse Width: Refers to the width of the Wiegand pulse in microseconds. The default value scope of the pulse width is 1–1000.

Pulse Interval: Refers to the interval of the Wiegand pulse in microseconds. The default value scope of the pulse width is 1–10000.

Output: Refers to the contents output upon successful verification. You can select the "User ID" or "Card Number" as the output.

5.2.1 Wiegand 26-bits Output Description

The system has a built-in Wiegand 26-bits format. Press [**Wiegand Format**], and select “Standard Wiegand 26-bits”.

The composition of the Wiegand 26-bits format contains 2 parity bits and 24 bits for output contents (“User ID” or “Card Number”). The binary code of 24-bits represent up to 16,777,216 (0–16,777,215) different values.

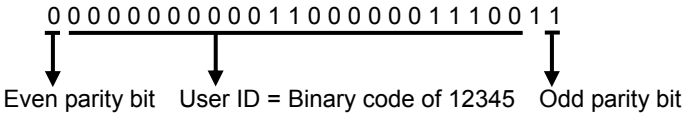
1	**2**	**25 26**
Even parity	User ID/Card Number	Odd parity bit

Definition of Fields:

Field	**Meaning**
Even parity bit	Judged from bit 2 to bit 13. The **even parity bit** is 1 if the character has an even number of 1 bits; otherwise, the even parity bit is 1.
User ID/ Card Number (bit 2-bit 25)	User ID/Card Number (Card Code, 0–16777215) Bit 2 is the Most Significant Bit (MSB).
Odd parity bit	Judged from bit 14 to bit 25. The **odd parity bit** is 1 if the character has an even number of 1 bits; otherwise, the odd parity bit is 0.

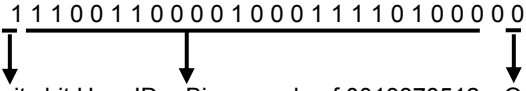
For example, for a user with user ID of 12345, the enrolled card number is 0013378512 and the failed ID is set to 1.

1. When the output is set to “User ID”, the Wiegand output is as follows upon successful verification:

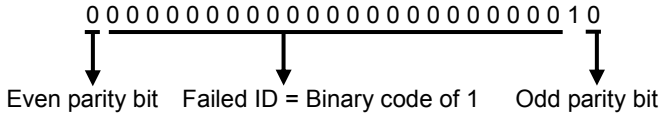


2. When the output is set to “Card Number”, the Wiegand output is as follows upon

successful verification:



3. The Wiegand output is as follows upon verification failure:



✍ **Note:** If the output contents exceed the scope allowed for the Wiegand format, the last several bits will be adopted and first several bits are automatically discarded. For example, the user ID 888 888 888 is 110 100 111 110 110 101 111 000 111 000 in binary format. Wiegand26 only supports 24 bits, that is, it only outputs the last 24 bits, and first 6 bits “110 100” are automatically discarded.

5.2.2 Wiegand 34-bits Output Description

The system has a built-in Wiegand 34-bits format. Press [**Wiegand Format**], and select “Standard Wiegand 34-bits”.

The composition of the Wiegand 34-bits format contains 2 parity bits and 32 bits for output contents (“User ID” or “Card Number”). The binary code of 32-bits represent up to 4,294,967,296 (0–4,294,967,295) different values.

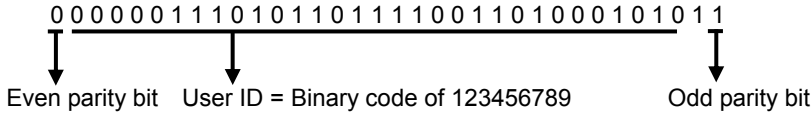
1	**2**	**33**	**34**
EvenParityBit	User ID/Card Number		Odd parity bit

Table 2 Definition of Fields

Field	**Meaning**
Even parity bit	Judged from bit 2 to bit 17. The **even parity bit** is 1 if the character has an even number of 1 bits; otherwise, the even parity bit is 1.
User ID/Card Number (bit 2-bit 33)	User ID/Card Number (Card Code, 0–4,294,967,295) Bit 2 is the Most Significant Bit (MSB).
Odd parity bit	Judged from bit 18 to bit 33. The **odd parity bit** is 1 if the character has an even number of 1 bits; otherwise, the odd parity bit is 0.

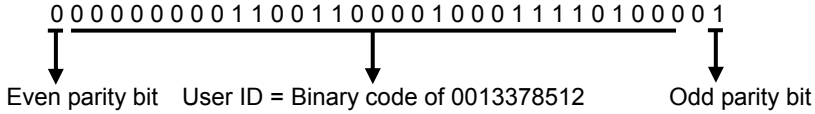
For example, for a user with user ID of 123456789, the enrolled card number is 0013378512 and the failed ID is set to 1.

1. When the output is set to “User ID”, the Wiegand output is as follows upon successful verification:

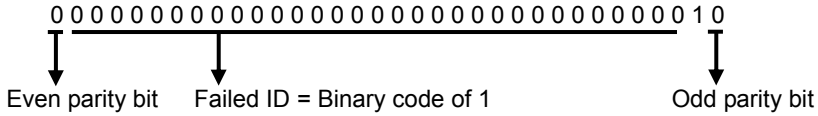


2. When the output is set to “Card Number”, the Wiegand output is as follows upon

successful verification:



3. The Wiegand output is as follows upon verification failure:



5.2.3 Customized Format

Apart from the two built-in formats **Wiegand 26-bits** and **Wiegand 34-bits**, the system also supports the format customization function to meet individualized requirements.

The customized format consists of two character strings: the **data bits** and **parity bits**. These two character strings need to be defined separately. **Data bits** define the number of binary bits output by Wiegand as well as the meaning of each bit. The data bits output by Wiegand can be a card number (C), site code (s), facility code (f), manufacturer code (m) and parity bits (p). **Parity bits** define the check mode of each bit in data bits and ensure the correctness of data bits during transfer through the parity check. The parity bits can be set to odd check (o), even check (e) and both odd check and even check (b). There exists a one-to-one correspondence relationship between the data bits and parity bits.

For example, the Wiegand26 can be customized as follows:

Definition of data bits: pssssssssccccccccccccccccp

Definition of parity bits: eeeeeeeeeeeeeooooooooooooo

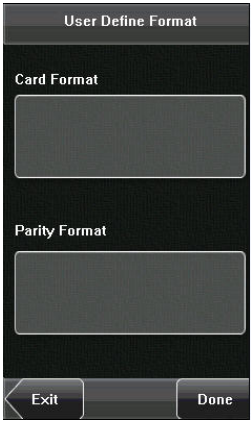
Note: Wiegand26 consists of 26 bits. The first bit is the even parity bit of bits 2 to 13; the 26th bit is the odd parity bit of bits 14 to 25; the second to the ninth bits are the site code; the 10th to the 25th bits are the card number.

For details about the Wiegand protocol, see Appendix 3 Introduction of Wiegand.

To customize Wiegand format, proceed as follows:

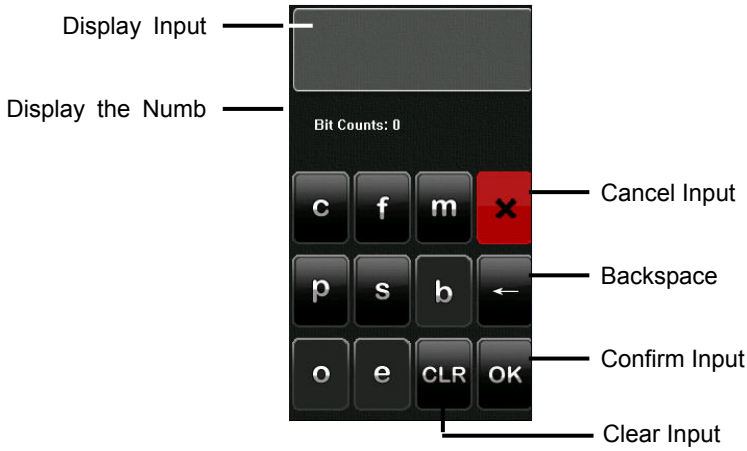
(1) Select [Define Format] and the [Set] key is then enabled.

(2) Press [Set] to display the [User Define Format]

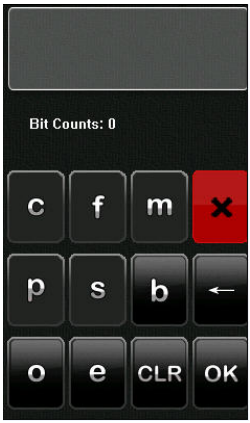


interface, as shown in the following figure:

(3) Click the entry box below “Card Format” to display the following interface:



Characters used to define data bits and their meanings:



c: Indicates the card number, that is, the output contents, it can be set to User ID/Card Number through menu operations.

f: Indicates the facility code which is 0 by default. It is not configurable. To modify it, please contact the equipment supplier.

m: Indicates the manufacturer code which is 0 by default. It is not configurable. To modify it, please contact the equipment supplier.

p: Indicates the parity position.

s: Indicates the site code which can be set from 0 to 255 by default.

(4) Click the entry box below “Parity Format” to display the following interface:

Characters used to define parity bits and their meanings:

o: Indicates the odd check, that is, there is an odd number of 1's in the bit sequence (including one parity bit). For example, for 1000110(0), the parity bit is 0 and there are already three 1's. After 0 is suffixed to 1000110, there is still an odd number of 1's.

e: Indicates the even check, that is, there is an even number of 1's in the bit sequence (including one parity bit). For example, for 1000110(1), the parity bit is 1 and there are already three 1's. After 1 is suffixed to 1000110, there is an even number of 1's.

b: Indicates both odd check and even check.

For example: Definitions of several universal Wiegand formats.

Wiegand34

Data bits:

pccccccccccccccccccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeoooooooooooooooo

Note: Wiegand34 consists of 34 bits. The first bit is the even parity bit of bits 2 to 17; the 34^{th} bit is the odd parity bit of bits 18 to 33; the second to the ninth bits are the site code; the 10^{th} to the 25^{th} bits are the card number.

Wiegand37a

Data bits: pmmmmsssssssssssscccccccccccccccccccp

Parity bits: oeobeobeobeobeobeobeobeobeobeobeobeoe

Note: Wiegand37a consists of 37 bits. The first bit is the odd parity bit of bits 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19, 21, 22, 24, 25, 27, 28, 30, 31, 33, 34 and 36; the 37^{th} bit is the odd parity bit of bits 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29, 31, 32, 34 and 35; bits 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 and 34 participate in both odd and even parity check. Bits 2 to 5 are manufacturer code; bits

6 to 17 are the site code; bits 18 to 36 are the card number.

Wiegand37

Data bits:

pmmmfffffffffssssscccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeeoooooooooooooooooo

Note: Wiegand37 consists of 37 bits. The first bit is the even parity bit of bits 2 to 18; the 34th bit is the odd parity bit of bits 19 to 36; the second to the fourth bits are the manufacturer code; the 5th to the 14th bits are facilitate code; the 15th to the 20th bits are the site code; the 21st to the 36th bits are the card number.

Wiegand50

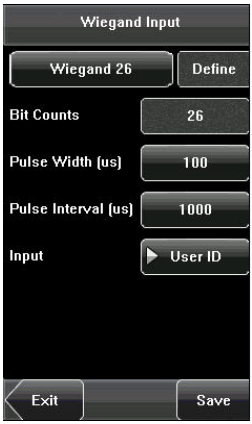
Data bits: pssssssssssssssscccccccccccccccccccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeeeeeeeeeooooooooooooooooooooooooo

Note: Wiegand50 consists of 50 bits. The first bit is the even parity bit of bits 2 to 25; the 50th bit is the odd parity bit of bits 26 to 49; the second to the 16th bits are the site code; the 17th to the 49th bits are the card number.

5.3 Wiegand Input



Wiegand Format: The system has two built-in formats **Wiegand 26-bits** and **Wiegand 34-bits**, and also supports the format customization function to meet individualized requirements. About the Wiegand format, please refer to 5.2 Wiegand Output.

Bit counts: Wiegand data digit length

Pulse width: Pulse width is 100 microseconds by default, which can be adjusted from 20 to 800.

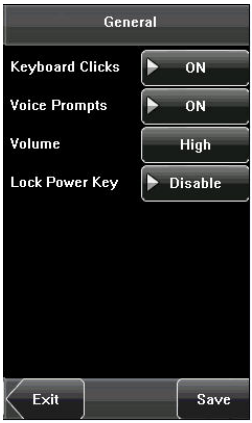
Pulse interval: It is 900 microseconds by default, which can adjusted between 200 and 20000.

Input: Content contained in Wiegand input signal, including User ID or card number.

6. System Configuration

Through the [System] menu, you can set system-related parameters, including the General, Display, Fingerprint, Face, Log settings, Shortcut Def, Access Control Set. and Firmware Update, to enable the device to meet user requirements to the greatest extent in terms of functions and display.

6.1 General Parameters



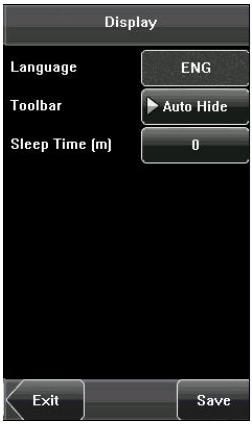
Keyboard Clicks: This parameter is used to set whether to generate beep sound in response to every keyboard touch. Select “ON” to enable the beep sound, and select “OFF” to mute.

Voice Prompts: This parameter is used to set whether to play voice prompts during the operation of the Device. Select “ON” to enable the voice prompt, and select “OFF” to mute.

Volume (%): This parameter is used to adjust the volume of voice prompts.

Lock Power Key: This parameter is used to set whether to lock the power key. Select “ON” to disable the power key. If you select “OFF” and press the power key, the Device will be shut down in three seconds.

6.2 Interface Parameters



Language: This parameter is used to display the current language used by the Device. For multilingual-capable Devices, you can switch between different languages through this parameter.

Toolbar: This parameter is used to display style of the shortcut keys on the initial interface. It can be set to "Auto Hide" and "Permanent Display". By selecting "Auto Hide", you can manually display or hide the toolbar. By selecting "Permanent Display", you can permanently display the toolbar on the initial interface.

Sleep Time (S): This parameter is used to specify a period after which the Device is put in sleep mode if not operated within this period. You can bring up the Device from sleep by pressing any key or touching the screen.

6.3 Fingerprint Parameters

1: 1 Threshold: This parameter is used to set the threshold of matching between current fingerprint and the fingerprint template enrolled in the device in the 1:1 verification mode. If the similarity between current fingerprint and the fingerprint template enrolled in the Device is larger than this threshold, the matching is successful; otherwise, the matching is not successful.

1: N Threshold: This parameter is used to set the threshold of matching between current fingerprint and the fingerprint template enrolled in the device in the 1:N verification mode. If the similarity between current fingerprint and the fingerprint template enrolled in the Device is larger than this threshold, the matching is successful; otherwise, the matching is not successful.

The recommended thresholds are as follows:

(FRR)	(FAR)	Threshold	
		1: N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Algorithm Version: This parameter is used to select the fingerprint algorithm version between 9.0 and 10.0. Please select the algorithm version with caution because the fingerprint templates of these two algorithm versions are incompatible.

Fingerprint Image: This parameter is used to set whether to display the fingerprint image on the screen during fingerprint enrollment or comparison. It has four values:

Show For Enroll: Display the fingerprint on the screen in enrolling process.

Show For Match: Display the fingerprint on the screen in verification process.

Always Show: Display the fingerprint on the screen in enrolling and verifying process.

Never Show: Never display the fingerprint on the screen in any case.

6.4 Face Parameters

1: 1 Threshold: This parameter is used to set the threshold of matching between current face and the face template enrolled in the Device in the 1:1 verification mode. If the similarity between current face and the face template enrolled in the Device is larger than this threshold, the matching is successful; otherwise, the matching is not successful. The valid value scope is 55─120. The higher the threshold, the lower the FAR and the higher the FRR, and vice versa.

1:1: N Threshold: This parameter is used to set the threshold of matching between current face and the face template enrolled in the Device in the 1:N verification mode. If the similarity between current face and the face template enrolled in the Device is larger than this threshold, the matching is successful; otherwise, the matching is not successful. The valid value scope is 65─120. The higher the threshold, the lower the FAR and the higher the FRR, and vice versa.

The recommended thresholds are as follows:

FRR	FAR	Threshold	
		1: N	1:1
High	Low	90	80
Medium	Medium	80	70
Low	High	75	65

Exposure: This parameter is used to set the exposure value of the camera.

Gain: This parameter is used to set the gain value of the camera.

Quality: This parameter is used to set a quality threshold for the face images obtained. The Device accepts the face images and processes them by adopting the

face algorithm when their quality is higher than the threshold; otherwise, it filters these face images.

✍ **Note:** Improper adjustment of the Exposure, Gain and Quality parameters may severely affect the performance of the Device. Please adjust the Exposure parameter only under the guidance of the after-sales service personnel from our company.

6.5 Log Settings

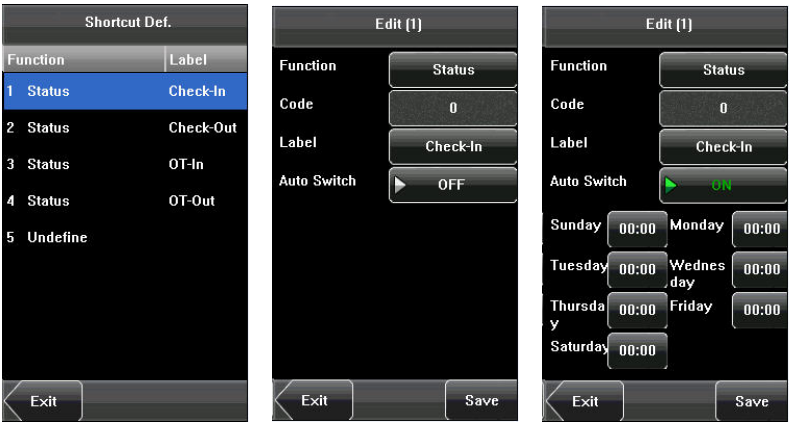
Log Alert: When the available space is insufficient to store the specified number of attendance records, the Device will automatically generate an alarm (Value scope: 1-99).

Dup. Punch Period (m): If a user's attendance record already exists and the user punches in again within the specified period (unit: minute), his/her second attendance record will not be stored (Value scope: 1-60 minutes).

6.6 Keyboard Definitions

Define touch screen functional shortcut keys.

1. Press [Shortcut Def] to display the [Edit] interface, as shown below.

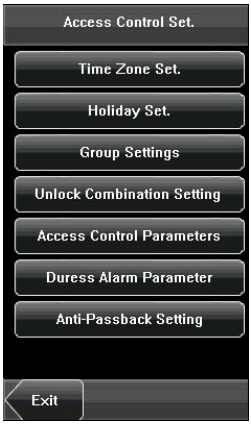


2. If you want to cancel the shortcut key, press [Status] to enter the edit interface, select the value to Undefine.

3. Edit the item [Code], select [Label] (Six attendance state option). Select if the state [Auto Switch] value, the interface shown as figure above.

4. Press [Save] to save the modification and exit.

6.7 Access Setting



Access control setting is to set user's open door time zone, control lock and related device's parameters.

To unlock, the enrolled user must accord with the following conditions:

1. The current unlock time should be in the effective time of user time zone or group zone.
2. The group where user is must be in access control (or in the same access control with other group, to open the door together).

The system default the new enrolled user as the first group, default group time zone as 1, access control as the first group, and the new enrolled user is in unlock (if user has modified the related setting of access control, the system will be changed with user's modification.)

6.7.1 Time zone setting

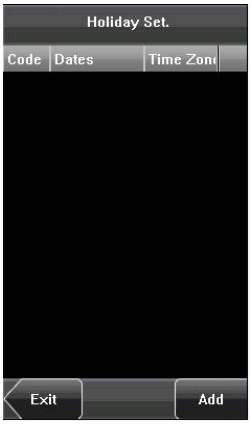
Time zone is the minimum unit of access control option. The whole system can define 50 time zones. Every time zone defines seven time sections (namely, a week). Every time section is the effective time zone within 24 hours everyday. Every user can set 3 time zones. “or” exists among the three zones. It is effective if only one is satisfied. Every time section format is **HH:MM-HH:MM**, namely, accurate to minute.

If end time is smaller than start time (23:57- 23:56), the whole day is forbidden. If end time is bigger than start time (00:00- 23:59), it is effective section.

Effective time zone for user unlocking:00:00-23:59 or end time is bigger than start time.

✍ **Notice:** System default time zone 1 as whole day open (namely, the new enrolled user is unlocking).

6.7.2 Holiday setting



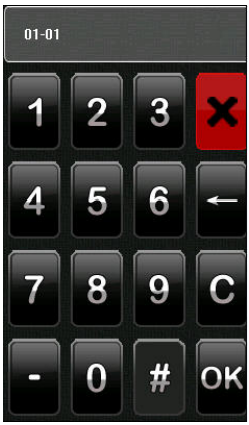
Special access control time may need during holiday. It is different to modify everybody's access control time. So a holiday access control time can be set, which is applicable for all employees.

1. Add holiday:

(1) Enter holiday add interface, press the key to edit the items.

(2) Press the touch screen number key to set the value, after setting, press [OK] to save, and press [X] for exit and return to previous interface.

(3) Press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.



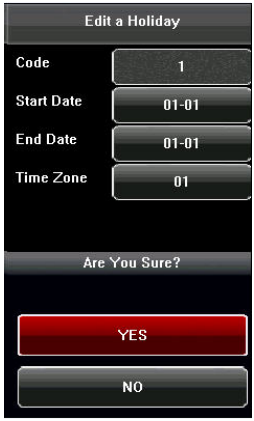
2. Edit holiday

Select the holiday to be edit and enter the edit interface. The edit operation is similar to add holiday. After edit, press [Save] to save and return to previous interface.

✍ **Notice**: If holiday access control time is set, user's open door time zone during holiday subject to the time zone here.

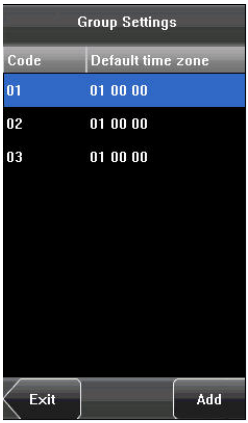
3. Delete holiday

Select the holiday to be deleted. Press **[Delete]** to popup the confirm interface as follows. Select [Yes] to delete this holiday, otherwise select [No] to cancel the operation.



6.7.3 Group time zone setting

Grouping is to manage employees in groups. Employee in groups use group time zone by default. Group members can also set user time zone. Every group can hold there time zones. The new enrolled user belongs to Group 1 by default and can also be allocated to other groups.



1. Add group time zone

(1) Enter the Add Group interface, press the key to edit the items.

Code: Enter the number edit interface to set the value.

VerType: Select the Group Verify Type.

Holiday No.: Select if the Time zone is valid in holiday.

Time Zone: Select the Group Time Zone.

(2) After editing, press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.

Note:

(1) RF means ID Card verification. Only the products with a built-in ID card module support the ID card verification.

(2) For Multi-combination verification please refer to Appendix 4 Multi-combination Authentication Mode.

Notice:

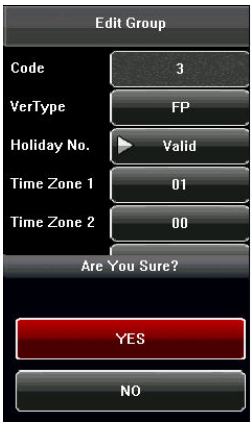
1. If holiday is effective, only when there is intersection between group zone and holiday time zone, can the group member open the door.
2. If holiday is ineffective, the access control time of group member won't be affected by holiday.

2. Edit group time zone

Select the line to be edited. Press **OK** directly or press **menu** to select **edit** in operating menu. After editing, press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.

3. Delete group time zone

Select the line to be deleted. Press **[Delete]** to popup the confirm interface as follows. Select [Yes] to delete this holiday, otherwise select [No] to cancel the operation.



6.7.4 Unlock Combination Setting

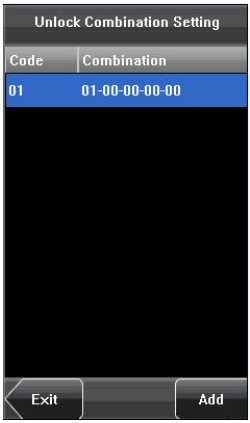
Make various groups into different access controls to achieve multi-verification and improve security. An access control can be made up of 5 groups at most.

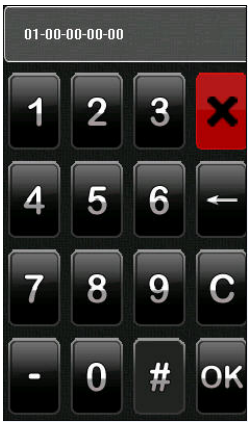
1. Add Unlock Combination

(1) Enter holiday add Combination Setting interface, press the key to edit the items.

(2) Press the touch screen number key to set the value, after setting, press [OK] to save, and press [X] for exit and return to previous interface.

(3) Press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.



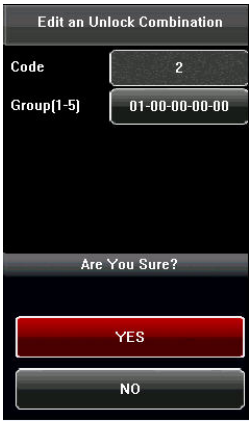


2. Edit Unlock Combination

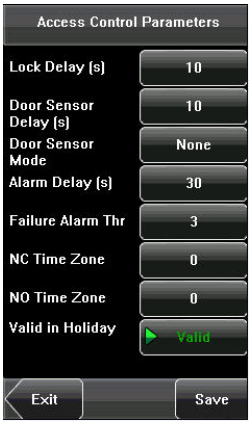
Select the line to be edited. Press **OK** directly or press **menu** to select **edit** in operating menu. After editing, press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.

3. Delete Unlock Combination

Select the line to be deleted. Press **[Delete]** to popup the confirm interface as follows. Select [Yes] to delete this holiday, otherwise select [No] to cancel the operation



6.7.5 Access control parameter



Through the [Access] menu, you can set the parameters of the electronic locks and related access control devices.

Lock Delay: indicates the duration for the Device to place the electric lock in open state. (Value scope: 1–10 seconds)

Door Sensor Delay: indicates the delay in checking the door sensor after the door is open. If door sensor state is inconsistent with the normal state set by the door sensor switch, an alarm will be generated, and this period of time is regarded as the “door sensor delay”. (Value scope: 1–99 seconds)

Door Sensor Mode: includes the None, Normally Open (NO), and Normally Closed (NC) modes. “None” indicates that the door sensor switch is not used. “NO” indicates that the door sensor is open in the normal state. “NC” indicates that the door sensor is closed in the normal state.

Alarm Delay: indicates the duration from the detection of door sensor exceptions to the generation of alarm signals. (Value scope: 1–99 seconds)

Failure Alarm Threshold: When the failed press times reach the set times, alarm signal will come out.(effective value 1～9 times)

NC Time Zone: Set time zone for access control NC. Nobody can unlock during this time zone.

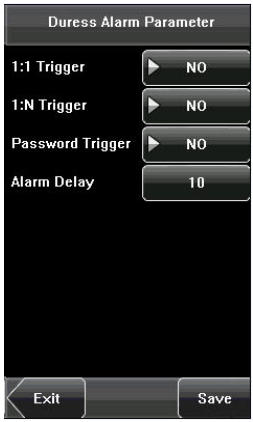
NO Time Zone: Set time zone for access control NO. The lock is always in enabling state during this time zone.

Valid in Holiday: Define time zone for NO or NC. Whether the time zone set in time zone is effective. **Notice**:1. When time zone is set for NO or NC, please set door sensor mode as None, or alarm signal may come out during time zone of NO or NC.

✍ **Notice**:

1. If the Time Zone of normally open or normally closed has been set, please switch door sensor to no, otherwise it will produce alarm signal during Normal close Time Zone or Normal open Time Zone .
2. If the normally open or normally closed Time Zone is not defined yet the time, the equipment will prompt that you define the Time Zone, and transferred to the Time Zone interface, to adding.

6.7.6 Duress alarm parameter



There is duress alarm parameter setting in the device. When employee come across duress, select duress alarm mode, the device will open the door as usual. But the alarm signal will be sent to the alarm.

1:1 Trigger: if select "Yes", when user use 1:1 match mode, alarm signal will come out. Or there is no alarm signal.

1:N Trigger: if select "Yes", when user use 1:N match mode, alarm signal will come out. Or there is no alarm signal.

Password Trigger: If select "Yes", when user use password verification mode, alarm signal will come out. Or there is no alarm signal.

Alarm Delay: After duress alarm gets started, the alarm signal is not output directly. But it can be defined. After some time, alarm signal will be generated automatically (0-255 seconds).

6.7.7 Anti-Pass back setting

Set the device Anti-Pass back function.

APB Direction: There are four options: None, APB-Out, APB-In, APB-Out/In.

Device Status: There are three options: Exit Control, Entry Control and none.

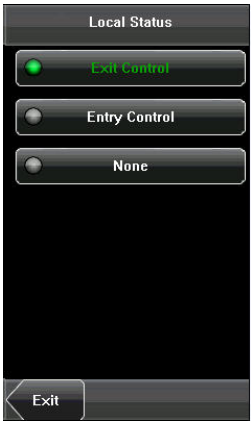
Anti-Pass back function please refer to Appendix 5 Anti-Pass back.

Anti-Pass back setting operation:

(1) Enter Anti-Pass back setting interface, press the key to edit the items.

(2) Press the touch screen number key to set the value, after setting, press [OK] to save, and press [X] for exit and return to previous interface.

(3) Press [Save] to save current information and return to previous interface; press [Exit] to directly return to previous interface without saving current information.



6.8 Update

You can upgrade the firmware program of the device by using the upgrade file in the USB disk through this function.

If you need the firmware upgrade file, please contact our technical support personnel. Generally the firmware upgrade is not recommended.

7. Data Management

Through the [Data Mgt.] menu, you can perform management of data stored on the device, for example, deleting the attendance record, all data and promotional pictures, purging management rights and resetting the device to factory defaults.

1. Delete Transactions: Delete all the attendance records.

2. Delete All Data: Delete all the information of enrolled personnel, including their fingerprints, face images and attendance records.

3. Clear Administrator: Change all administrators to ordinary users.

4. Restore to Factory Settings: Restore all parameter settings on the device to factory settings.

Notice: The employee information and attendance records will not be deleted during restoration to factory settings.

5. Query Record: After check-in successfully, the employee's attendance records are saved in the device. You can easily query these attendance records.

User ID: Enter the user ID of the employee to query. If this field is left blank, you can query the attendance records of all the employees. If you enter a user ID, you can query the attendance record of the employee with this user ID.

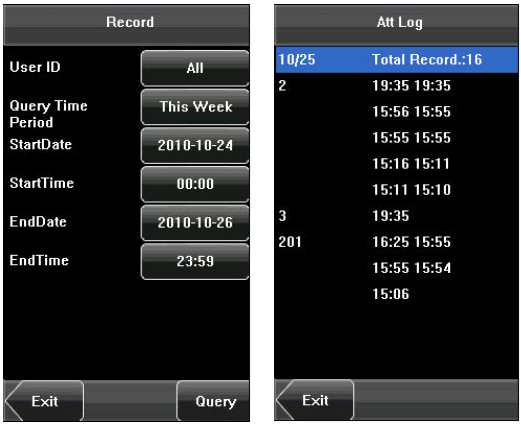
Query Time Period: Select a time period to query, including the customized time

period, yesterday, this week, last week, this month, last month, and all time periods.

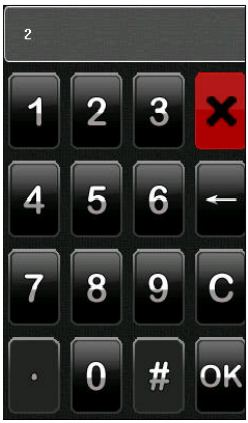
Start and **End**: When you select a customized time period, you need to input a start time and an end time. When you select other options for time period, the start and end time will be automatically adjusted to the related time.

After setting the query conditions, press [Query] and the records that meet the specified query conditions will be displayed on screen.

Select the row where the desired record is located, you can query the detailed information of this records.



Press User ID and enter the edit interface, input the ID number and press [Query], the query result will display as below.


2
1
2
3
4
5
6
7
8
9
C
0
#
OK

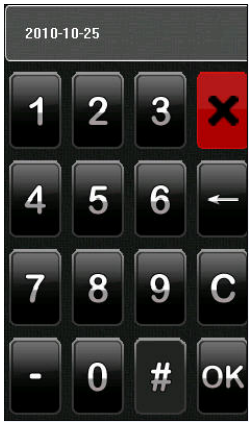
Att Log(User ID:2)
10/25 19:35 19:35
15:56 15:55
15:55 15:55
15:16 15:11
15:11 15:10
Exit

8. Date/Time Setting

8.1 Set Date/Time

The date and time of the device must be set accurately to ensure the accuracy of attendance time.

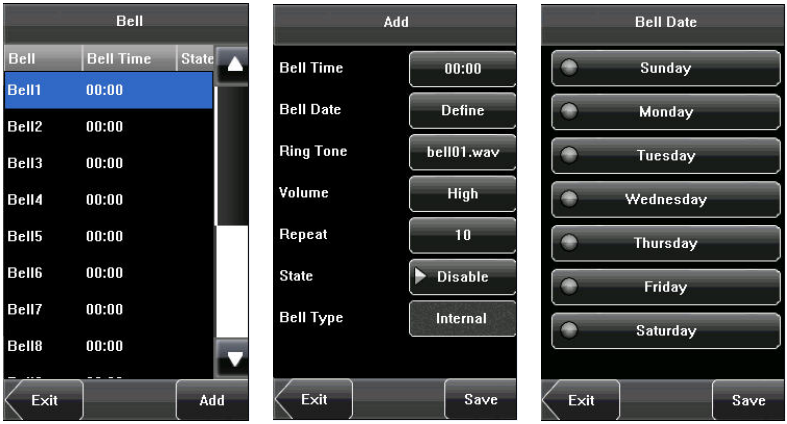
1. Press [**Menu**] on the initial interface to display the main menu interface.
2. Press [**Time/Date**] on the main menu interface to display the time setting interface.
3. Select the desired date and time by pressing the parameter. For the time format, there 10 format to select. Both the 12-hour and 24-hour time systems are supported.
4. Press [**Save**] to save current information and return to the previous interface. Press [**Exit**] to return to the previous interface without saving current information.



8.2 Bell Setting ★

Lots of companies need to ring their bells to signal the start and end of work shifts, and they usually manually ring their bells or use electric bells. To lower costs and facilitate management, we integrate the time bell function into the device. You can set the alarm time and duration for ringing the bell based on your requirements, so that the device will automatically play the selected ring tone and trigger the relay at the alarm time, and stop playing the ring tone after the set duration.

Press [**Bell**] on the [Date/Time] menu to display the bell setting interface, as shown in Figure below.



1. Add a bell

1) The displayed bell setting interface lists all the bells. Click [Add] to display the [Add] interface.

2) On the [Add] interface, set the following parameters:

Bell Time: This parameter is used to set a time point when the Device automatically plays a bell ring tone everyday.

Bell Date: This parameter is used to set which day the device automatically plays a bell ring tone.

Ring Tone: This parameter is used to set the bell ring tone.

Volume: This parameter is used to set the volume of ring tone.

Repeat: This parameter is used to set the alarm times.

State: This parameter is used to set whether to enable the bell.

Bell Type: You can select between internal ringing or external ringing. For internal ringing, the ring tone is played by the loudspeaker of the device. For external ringing, the ring tone is played by an external electric bell that is wired with the device.

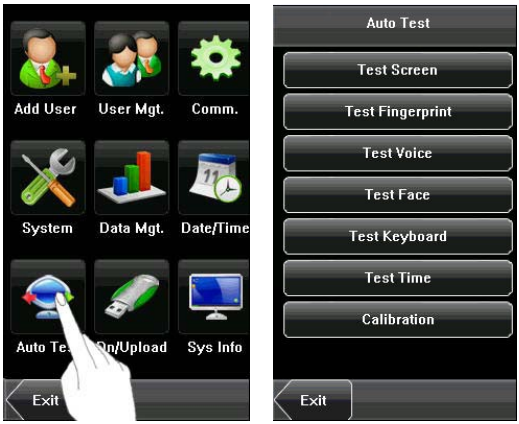
2. Edit and delete a bell

Press a bell in the list on the bell setting interface to display the [**Edit**] interface, with the similar operation as "Add a bell".

✍ **Notice**: Only some models have this function. If you need it, please contact our business representative or technician.

9. Auto Test

The auto test enables the system to automatically test whether functions of various modules are normal, including the screen, collector, voice, face, keyboard and clock tests.



1. Test Screen: The device automatically tests the display effect of the color TFT display by displaying full color, pure white and pure black and checks whether the screen displays properly. You can continue the test by touching the screen or exit it by pressing [Exit].

2. Test Fingerprint: The device automatically tests whether the fingerprint collector works properly by checking whether the fingerprint images are clear and acceptable. When the user places his/her finger in the fingered guide, the collected fingerprint image is displayed on the screen in real-time. Press [Exit] to exit the test.

3. Test Voice: The device automatically tests whether the voice files are complete and the voice quality is good by playing the voice files stored in the device. You can continue the test by touching the screen or exit it by pressing [Exit].

4. Test Face: The device automatically tests whether the camera works properly by

checking whether the collected face images are clear and acceptable. Press [Auto Test] to exit the test.

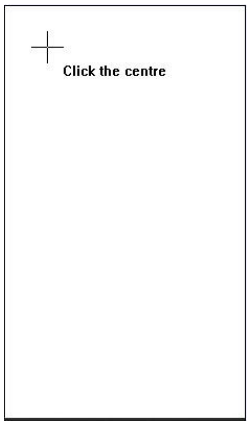
5. Test Keyboard: The device tests whether every key on the keyboard works normally. Press any key on the [Keyboard Test] interface to check whether the pressed key matches the key displayed on screen. The keys are dark-gray before pressed, and turn blue after pressed. Press [Exit] to exit the test.

6. Test Time: The device tests whether its clock works properly by checking the stopwatch of the clock. Touch the screen to start counting, and touch it again to stop to check whether the counting is accurate. Press [Exit] to exit the test.

7. Screen Calibration:

You can perform all the menu operations by touching the screen with one of your fingers or a touch pen. When the touch screen is less sensitive to the touch, you can perform screen calibration through menu operations.

The Screen Calibration Operation:



(1) Press [Menu] on the initial interface to display the main menu interface.

(2) Press [Calibration] on the [Auto Test] interface to display the screen calibration interface.

(3) Touch the center of the cross “+”.

(4) Repeat Step 3 following the move of the “+” icon to different locations on the screen.

(5) Touch the center of the cross at five locations on the screen correctly. When the message “Calibrating screen, pls wait……” is displayed on screen, the calibration succeeds and the system automatically returns to the main menu. If the calibration fails, the system will request recalibration starting from Step 3.

10. USB Disk Management

Through the [**Dn/Upload**] menu, you can import user information and attendance data stored in a USB disk to related software or other fingerprint recognition equipment.

1. Download Transactions: Import all the attendance data from the device to a USB disk.

2. Download User: Import all the user information, fingerprints and face images from the device to a USB disk.

3. Download user photos: Import the employees' photos from the device to a USB disk.

4. Upload User: Upload the user information, fingerprints and face images stored in a USB disk to the device.

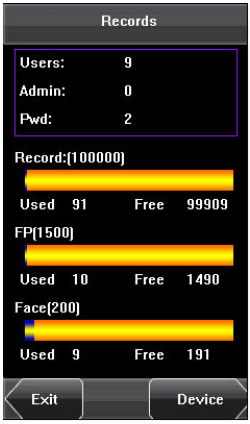
5. Upload User Photo: Upload the JPG documents that are named after the user IDs and stored in a USB disk to the device, so that user photos can be displayed after the employees pass the verification. See Appendix 3 Photo ID Function.

11. System Information

You can check the storage status as well as version information of the device through the [System Information] option.

Records: The number of enrolled users, administrators and passwords is displayed on the [**Records**] interface; the total fingerprint storage capacity and occupied capacity as well as the total attendance storage capacity and occupied capacity are graphically displayed respectively.

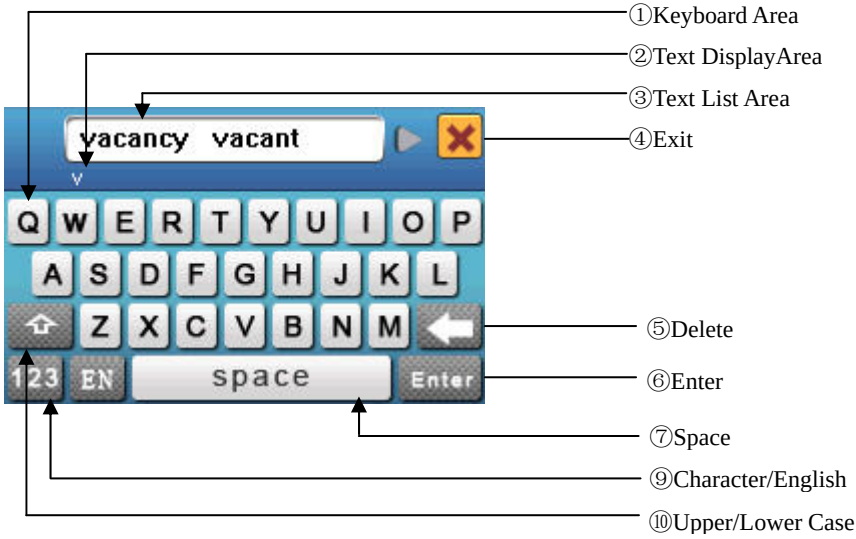
Device: The device name, serial number, version information, vendor and date of manufacture are displayed on the [**Device**] interface.



12. Appendix

Appendix 1 T9 Input Instructions

The Device supports the input of English characters, numbers and symbols. Press related button to input text. For example, press [Name] to display the text input interface, as shown in the figure:



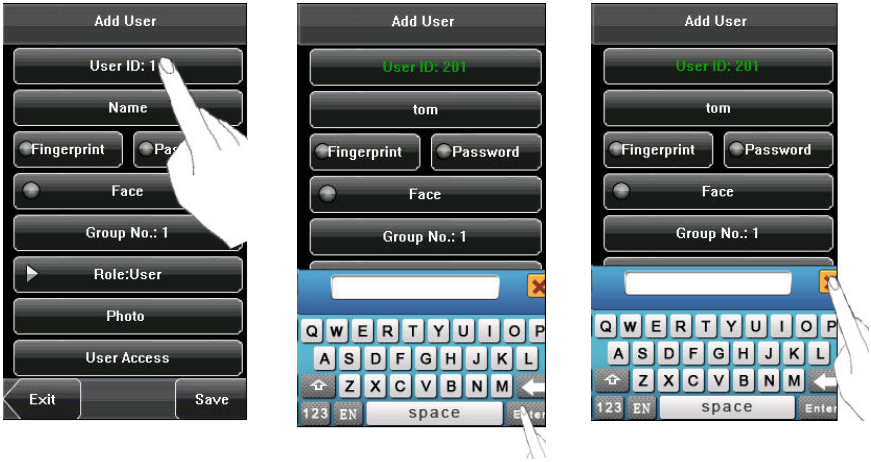
To enter a name, proceed as follows:

1. Press [Name] on the [Add] interface, as shown in Figure below.

2. Enter the letter characters, and a list of characters in relation to the letter is presented in the text display area.

3. If the desired character is displayed in the text display area, press this character. And this character is at the same time displayed on the [Name] button. Enter next character by repeating Step 2.

4. After finishing the entry of name, press [X] to exit keyboard interface and return to the previous interface.



Appendix 2 Introduction of Wiegand

Wiegand26 is an access control standard protocol established by the Access Control Standard Subcommittee affiliated to the Security Industry Association (SIA). It is a non-contact IC card reader interface and output protocol.

Wiegand26 defines the interface between the card reader and controller used in the access control, security and other related industrial fields. Wiegand26 helps standardize the work of the card reader designers and controller manufacturers. The access control products manufactured by our company are also designed by following this protocol.

Digital Signals

The figure below is a sequence diagram in which the card reader sends digital signals in bit format to the access controller. In this sequence diagram, Wiegand follows the SIA's access control standard protocol for the 26-bit Wiegand card reader (one pulse time ranges between 20us and 100us, and the pulse jump time ranges between 200us and 20ms). Data1 and Data0 are high level (larger than Vol) signals till the card reader prepares to send a data stream. The asynchronous low-level pulse (smaller than Vol) generated by the card reader is sent to the access control panel (The saw-tooth wave as shown in Figure below) through Data1 or Data0. Data1 and Data0 pulses will neither overlap nor be generated synchronously. The table below lists the maximum and minimum pulse width (a consecutive pulse) and pulse jump time (time between pulses) allowed by the F series fingerprint access control device.

Figure: Sequence Diagram

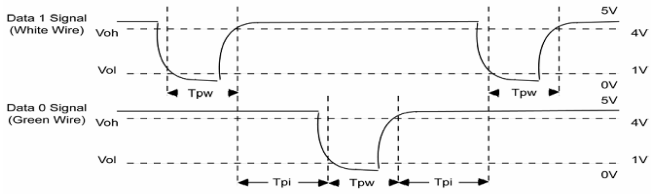


Table: Pulse Time

Symbol	Definition	Typical Value of Reader
Tpw	Pulse Width	100 μs
Tpi	Pulse Interval	1 ms

Appendix 3 Photo ID Function

Some Devices also support the Photo ID function. The Photo ID function is used to display the photo enrolled by a user or stored in a USB disk on the screen in addition to such information as the user ID and name.

[Operation Steps]

1. When the photo taken by the device is used, the photo can be displayed upon successful verification.

2. To use a photo stored in a USB disk, proceed as follows:

1) Create a folder with the name of “photo” in the USB disk, and store users' photos under this folder.

2) The user photos must be in JPG format and named after their IDs. For example, for the user with user ID of 154, the photo name must be 154.jpg.

3) Insert the USB disk into USB slot on the device, and select USB Disk Management -> Upload -> Upload Photos. Then user photos can be displayed upon successful verification.

Note:

1) The length of a user name cannot exceed 24 digits.

2) The recommended size of a user photo is less than 30kbit.

3) The uploaded new user photo will overwrite the existing photo in related to the user ID.

4) To download user photos, select USB Disk Management -> Download -> Download User Photos. A folder with the name of “photo” will be automatically created on the USB disk, and all downloaded user photos are stored under this folder.

Appendix 4 Multi-combination Authentication Mode ★

Besides this function only is owned by the fingerprint access control machine that has been appointed, the most fingerprint machine only has two way to verified by fingerprint and password, we provide a personal or group Multi-combination Authentication Mode for high security Access control area, verification type main include five elements that are User Number (PIN), Fingerprint (FP), Face (FACE), Password (PW) and RF card (RF), which can combine into multi-combination.

✍ **Note**: The RF card is used for ID Card verification, the function of ID card verification only is validity in the machine which ID card function is provided with.

These symbols illustrate what follow the table different means.

- **"/" is or**
- **"+" follow next operation**
- **"&" is and**
- **FACE (Face)**
- **FP (fingerprint)**
- **PWD (Password)**
- **RF (RF card)**
- **PIN (user ID)**

If Fingerprint, Face, Password and Card has been used to enroll user, the verification procedure is follow.

Type	What you do
FACE&PIN/FP/PW/RF	FACE+PIN or RF or PW or RF is verified
	1) PIN++FACE(1:1) 2) FP(1:N) 3) PIN+PW+"OK" 4) RF(1:N)
FP&PW	FP + PW are verified
	1) FP(1:N)+PW+"OK"

	2) PIN+FP(1:1)+PW+“OK” 3) PIN+PW+“OK”+FP
FP&RF	FP and RF are verified
	1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)+RF
FACE&FP	FACE + FP are verified 1) FP(1:N)+FACE 2) FACE(1:N)+FP 3) PIN+FACE(1:1)+FP 4) PIN+FP(1:1)+FACE
FACE&PW	FACE + PW are verified
	1) FACE(1:N)+PW+“OK” 2) PIN+FACE(1:1)+PW 3) PIN+PW+FACE
FACE&RF	FACE + RF are verified
	1) FACE(1:N)+RF 2) PIN+FACE(1:1)+RF 3) RF(1:N)+FACE
FP	Only FP is verified.
	1) PIN+FP(1:1) 2) FP(1:N)
PW	Only verify PW is verified
	PIN+PW+“OK”
RF	Only RF is verified
	RF(1:N)
FACE&PIN	FACE + PIN are verified PIN+FACE(1:1)

FP/RF	FP or RF is verified
	1) PIN+FP(1:1) 2) RF(1:N) 3) FP(1:N)
PW/RF	FP or RF is verified
	1) PIN+PW+“OK” 2) RF(1:N)
FP/PW	FP or PW is verified
	1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+PW+“OK”
PIN&FP	PIN + FP are verified
	PIN+FP(1:1)
FP&PW&RF	FP + PW + RF are verified
	1) FP(1:N)+PW+“OK”+RF 2) PIN+FP(1:1)+PW+“OK”+RF 3) RF(1:N)+PW+“OK”+FP 4) PIN+ PW+“OK”+FP(1:1)+RF
PIN&FP& PW	PIN + FP + PW are verified
	1) PIN+PW+“OK”+FP(1:1) 2) PIN+FP(1:1)+PW+“OK”
FP & RF/PIN	FP + PIN, or FP + RF are verified
	1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)
FACE&FP&RF	FACE + FP + RF are verified 1) FACE(1:N)+FP+RF 2) FP+FACE(1:1)+RF

	3) RF(1:N)+FACE+FP 4) PIN+FP(1:1)+FACE+RF 5) PIN+FACE(1:1)+FP+RF
FACE&FP&PW	FACE + FP + PW are verified 1) FACE(1:N) +PW+“OK”+FP 2) FP+PW+“OK”+FACE(1:1) 3) PIN+FP(1:1) +PW+“OK”+FACE 4) PIN+FACE(1:1) +PW+“OK”+FP 5) PIN+PW+“OK”+FP+FACE

✍ **Note:** For combined verification, it is better to enroll all the elements in need of the using verification mode, or verification will fail.

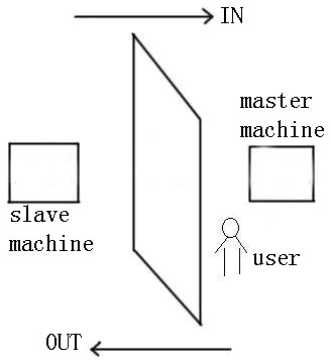
For example: User A use fingerprint for enrollment, while password is used for verification, then the user cannot pass the verification.

Appendix 5 Anti-Pass Back ★

【overview】

Sometimes, some illegal person follows the other one into the gate, which will bring security problem. To prevent such risk, this function is enabled. In record must match out record, or the gate won't be open.

This function needs two machines to work together. One is installed inside the door (master machine hereinafter), the other is installed outside the door (slave machine hereinafter). Wigand signal communication is adopted between the two machines.



【working principle】

The master machine has Wigand In and slave machine has Wigand Out. Connect Wigand Out of slave machine to Wigand In of master machine. Wigand output from slave machine must not own machine ID. The number sent to master machine from slave machine must be found in the master machine.

【function】

Judge whether it is anti-pass back according to user's recent in-out record. In record and out record must be matched. This machine supports out, in, or

out-in anti-pass back.

When master machine is set as “out anti-pass back”, if user wants to come in and go out normally, his recent record must be “in”, or he cannot go out. Any “out” record will be “anti-pass back refused”. For example, a user’s recent record is “in”, his second record can be “out” or “in”. His third record is based on his second record. Out record and in record must match.（Notice: If customer has no record before, then he can come in but cannot go out.)

When the master machine is set as “in anti-pass back”, if the user wants to come in and go out normally, his recent record must be “out”, or he cannot go out. Any out record will be “anti-pass back refused” by the system. (Notice: If the customer has no former record, then he can go out, but cannot come in.)

When the master machine is set as “out-in anti-pass back”, if the user wants to come in and go out normally, if his recent record is “out” and “in”, then his next record must be “ in” and “out”.

【operation】

1. Select model

Master machine: Machine with Wiegand in function, except for F10 reader.

Slave machine: Machine with Wiegand Out function.

2. Menu setting

Anti-pass back

There are four options: in/out anti-pass back, out anti-pass back, in anti-pass back, and none.

Out anti-pass back: Only user’s last record is in-record, can the door be open.

In anti-pass back: Only user’s last record is out-record, can the door be open.

Device status

There are three options: Control-in, control-out and none

Control-in: When it is set, the verified record on the device is in-record.

Control-out: When it is set, the verified record on the device is out-record.

None: When it is set, close the device's anti-pass back function.

3. Modify device's Wiegand output format

When the two devices are communicating, only Wiegand signals without device ID are received. Enter device menu－> communication option－> Wiegand option or enter software -〉basic setting -〉device management -〉 Wiegand, to modify "defined format" as "wiegand26 without device ID".

4. Enroll user

The user must be on master machine and slave machine at the same time, and user PIN must be the same. Therefore, it is necessary to enroll user on master machine and slave machine at the same time.

5. Connection instruction

Wiegand communication is adopted for master machine and slave machine. Refer to the following for connection:

Master		Slave
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

Appendix 6 Statement on Human Rights and Privacy

Dear Customers:

Thank you for choosing the hybrid biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.

We hereby make the following statements:

1. All of our fingerprint recognition devices for civil use only collect the characteristic points of fingerprints instead of the fingerprint images, and therefore no privacy issues are involved.
2. The characteristic points of fingerprints collected by our products cannot be used to restore the original fingerprint images, and therefore no privacy issues are involved.
3. We, as the equipment provider, shall not be held legally accountable, directly or indirectly, for any consequences arising due to the use of our products.
4. For any dispute involving the human rights or privacy when using our products, please contact your employer directly.

Our fingerprint products for police use or development tools support the collection of the original fingerprint images. As for whether such a type of fingerprint collection constitutes an infringement of your privacy, please contact the government or the final equipment provider. We, as the original equipment manufacturer, shall not be held legally accountable for any infringement arising thereof.

The law of the People’s Republic of China has the following regulations regarding the personal freedom:

1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.
2. The personal dignity of citizens of the People's Republic of China is inviolable.

3. The home of citizens of the People's Republic of China is inviolable.
4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.

At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The biometric products actually provide adequate protection for your identity under a high security environment.

Appendix 7 Environment-Friendly Use Description

The Environment Friendly Use Period (EFUP) marked on this product refers to the safety period of time in which the product is used under the conditions specified in the product instructions without leakage of noxious and harmful substances.

The EFUP of this product does not cover the consumable parts that need to be replaced on a regular basis such as batteries and so on. The EFUP of batteries is 5 years.

Names and Concentration of Toxic and Hazardous Substances or Elements

Parts Name	Toxic and Hazardous Substances or Elements					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	×	○	○	○	○	○
Chip capacitor	×	○	○	○	○	○
Chip inductor	×	○	○	○	○	○
Chip diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.

Note: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.